UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,871,276 B1
APPLICATION NO. : 09/543056
DATED : March 22, 2005
INVENTOR(S) : Simon

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 1, line 51, after "For" delete "to".

In column 4, line 41, after "circuits" insert -- (ASICs). --.

In column 8, line 58, delete "$M_{encrypt}=m^e(\mathrm{mod}\ n)$" and insert -- $m_{encrypt} = m^e(\mathrm{mod}\ n)$ --, therefor.

In column 8, line 67, delete "M_{ecrypt}" and insert -- $m_{encrypt}$ --, therefor.

In column 10, line 33, delete "Table 1" and insert -- Table **I** --, therefor.

In column 10, line 52, delete "Table 1" and insert -- Table **I** --, therefor.

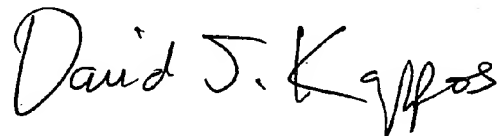In column 13, line 19, after "for" delete ",".

In column 14, line 13, in Claim 1, delete "where" and insert -- wher**ein** --, therefor.

In column 15, line 11, in Claim 5, after "integer" delete "," and insert -- ; --, therefor.

In column 16, line 4, in Claim 6, delete "band" and insert -- ba**sed** --, therefor.

Signed and Sealed this

Twenty-ninth Day of September, 2009

David J. Kappos
Director of the United States Patent and Trademark Office